Taking Charge of Your Privacy

What steps can you take now to protect your privacy online?

- **Use two-factor authentication** on every app that offers it.
- **Install VPN software** on your personal computers and smartphone. This hides your browsing habits and protects you from fraudsters who try to access your phone when you're on a Wi-Fi network.
- Also **install antivirus and anti-malware apps** on your personal devices.
- Review every app on your phone and **turn off "location settings"** except for apps you use regularly that require location information, such as Waze for traffic conditions, weather and apps that provide directions.
- **Review and understand privacy settings** on your social media accounts, particularly Facebook and WhatsApp. As *Fast Company* says, "you can't have privacy and use Facebook."
- *Fast Company* also recommends **using a search engine other than Google**, because Google's business model (like Facebook's) generates profit by knowing what you do online.
- Be careful **not to post identifying information about your family and work** on social media accounts. Fraudsters are skilled at combining facts about people to impersonate them online.
- **Don't accept friend requests from people you don't know** (even on LinkedIn), and don't allow anyone to follow you on Twitter.
- Go to your Google account and **run a "privacy checkup."**
- Remember, while Gmail is secure, it **indexes all the text in emails you send and receive** in order to serve up relevant advertising as you surf the web.
- Don't use **social media accounts to log in** to other websites.
- **Check out as a "guest"** when you purchase something on an e-commerce site where you don't shop frequently.
- For messaging, **use Signal or Apple's Messages** app instead of Facebook Messenger or WhatsApp.
- Remember, **everything you post online creates a digital trail about you**, and it will live on the web forever.